Weak Password Recovery Mechanism for Forgotten Password in chamilo/chamilo-lms (<=1.11.36 & 2.0-RC.2)

Critical **ywarnier** published **GHSA-f27g-66gq-g7v2** 5 hours ago

Package

php **chamilo/chamilo-lms** (Composer)

Affected versions	Patched versions
<= 1.11.36, 2.0-RC.2	1.11.38, 2.0-RC.3

Description

Summary

The default password reset mechanism generates tokens using `sha1($email)` with no random component, no expiration, and no rate limiting. An attacker who knows a user's email can compute the reset token and change the victim's password without authentication.

Details

Affected code: `main/inc/lib/login.lib.php`

Token generation (Line 251-254):

```
public static function get_secret_word($add)
{
    return $secret_word = sha1($add);  // $add = user's email
}
```

Token validation (Line 288) -- no expiration check:

```
if (self::get_secret_word($user['email']) == $secret) {
    $user['password'] = api_generate_password();
    UserManager::updatePassword($id, $user['password']);
}
```

Reset URL format: `lostPassword.php?reset={SHA1_OF_EMAIL}&id={USER_ID}`

This vulnerable path is the **default** -- active when `user_reset_password` setting is `'false'` (default in `main/install/data.sql` line 1785).

Issues:

1. Token = `sha1(email)` -- completely deterministic
2. No expiration -- works forever, even without requesting a reset first
3. No rate limiting -- unlimited attempts
4. Loose comparison `==` instead of `===` or `hash_equals()`
5. User ID is sequential and guessable

Impact

- Account takeover for any user whose email is known
- Token never expires and requires no prior reset request
- Combined with `get_user_info_from_username` (which exposes emails), enables full attack chain:
  - Discover email via REST API → compute sha1(email) → reset password → account takeover

Severity

Critical 9.4 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	Low

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

CVE ID

CVE-2026-33707

Weaknesses

▶ CWE-640

Credits

8l4nnk Reporter